CYBER INSURANCE MARKET WATCH SURVEY EXECUTIVE SUMMARY

October 2015

THE COUNCIL

The Council of Insurance Agents & Brokers

About The Survey

The Council of Insurance Agents & Brokers (The Council) represents the nation's leading insurance brokers who collectively place 85 percent of U.S. commercial property/casualty premiums annually. During September 2015, The Council fielded its first official Cyber Insurance Market Watch survey. The purpose of this biannual survey is to provide a retrospective snapshot of the cyber insurance market over the past six months from a nationwide sample of brokers. As the market develops over time, this survey will evolve into a market index similar to The Council's commercial property/casualty index which is the industry's gold standard and leading baseline of market conditions, pricing practices and trends.

Although there are a number of surveys generated by various insurance industry stakeholders, this survey differentiates itself by the fact that The Council's members are uniquely positioned to understand the development of the cyber insurance market from both the buy side and the sell side. Brokers' insights into how their clients are - or are not - approaching cyber insurance is a unique barometer of cybersecurity in the U.S., particularly within the private sector. The thinking of many is that insurance will act as a catalyst for companies to become better at cyber risk assessment and information security in exchange for lower premiums and higher liability limits.

The survey collected information from 75 cyber experts working at 53 unique insurance brokerages from across the country. These brokerages range from regional agencies to the largest global brokers, wholesale and retail, whose clients range from small and medium-sized businesses to Fortune 100 companies across all industries. These brokers are on the front lines of educating clients about their tangible and intangible asset risks and coordinate insurance coverage, risk management programs, compliance and claims. We posed 12 qualitative and quantitative questions. The majority of questions included an open response box for brokers to give personal anecdotes and insights into the market, which allowed us to take a look under the hood of how the insurance market is responding to this new breed of risk. The following executive summary downloads the highlights of the survey. The in-depth findings are exclusive to survey participants.

The Cyber Insurance Market

It is worth beginning with some background on how the cyber insurance marketplace has developed since its inception in the late 1990s. Cyber coverage has evolved from a tech errors and omission (E&O) policy covering mainly information technology professionals to a stand-alone cyber risk insurance market. The first iterations of today's "cyber" policies appeared when the rise of the internet and e-commerce spurred the industry to develop "internet insurance" policies which were limited to responding only to security failures of an insured's computer system. They did not provide coverage for first-party costs of mitigating a data breach nor did they extend coverage to non-electronic records or accidental disclosure.[1]

Early policies began to develop into the first generation of cyber products we know today around the mid-2000s with the addition of "privacy incidents" being added to coverages. These modifications expanded policies' "response to accidental disclosure of sensitive data in both electronic or paper form; liability coverage was expanded beyond civil actions to also include regulatory investigations; coverage started to appear for contractual fines paid to payment card brands for security non-compliance (contractual liability being generally excluded by E&O policies);

[1] Rob Jones, "Cyber Insurance: What You Should Know," in Symantec's Industry Experts Report: What Every CISO Needs to Know About Cyber Insurance, October 27, 2015, http://www.symantec.com/content/en/us/enterprise/white_papers/what-every-ciso-needs-to-know-cyber-insurance-21359962-wp.pdf.

and new first-party coverages were created to respond to the costs of investigating and mitigating a security or privacy incident." [2]

Along the way, insurance buyers found some protection in various other commercial insurance policies, including professional liability, crime and property and general liability. However, today the market is moving away from a reliance on embedded coverage towards a stand-alone cyber risk insurance market. For example, insurers are moving towards excluding cyber risk coverage from commercial general liability (CGL) policies. While existing forms carry a level of coverage, they were not intended to cover many risks in the digital world.

Currently, "most insurers offer cyber policies with coverage on an a la carte basis; a company can choose which coverages are right for it. The main coverage components are: defense and indemnity for alleged liability due to cyber or a privacy incident ('Liability'); coverage for investigating and mitigating a cyber or privacy incident ('Event Response'); coverage for business interruption due to a cyber incident ('Business Interruption') and coverage for the response to threats to harm a network, or release confidential information ('Cyber Extortion')." [3]

It is important to note that the vast majority of these cyber policies exclude three key types of loss: tangible property, bodily injury and loss of company's funds. It remains to be seen how these will be addressed by insurers who are grappling with a lack of information in order to understand a client's cyber risk profile and profitably assume risk. No one is immune from cyber risk and each company's risk profile is different depending on the business size and scope, so it's a challenge.

However, this isn't the first new emerging risk or the last for the insurance industry. There will be "brittle" periods but where there is an appetite for this coverage, solutions will follow. What is considered core coverage today was not available three years ago, and creative approaches are being deployed every day to seek access to more information, make enhancements and advance the cyber insurance market.

Survey Highlights

Cyber Insurance Buyer Behavior

The U.S. remains mostly uninsured when it comes to cybersecurity. The average take up rate for cyber insurance is 24 percent across U.S. business.

Overall, cyber insurance take up rates are increasing for all sized businesses, but at a fairly slow pace in the small and medium-sized business segment. The majority of survey participants noted that it is still difficult to sell cyber insurance to most small and medium-sized businesses despite increased educational efforts and a national media spotlight on cybersecurity. These businesses still have a mindset that because they are smaller or don't store personally identifiable information; they're not likely to be a victim of cybercrime. One broker stated, "quit using Sony and Target as examples because they're Fortune 500 companies and their exposures don't resonant with typical clientele."

[2] Jones, "Cyber Insurance: What You Should Know," in Symantec's Industry Experts Report: What Every CISO Needs to Know About Cyber Insurance.
[3] Jones, "Cyber Insurance: What You Should Know," in Symantec's Industry Experts Report: What Every CISO Needs to Know About Cyber Insurance.

Thirty-three (33) percent of survey participants said that clients who have basic protection for network and data breaches sought additional coverage(s) at renewal during the last six months.
The reasons for purchasing more cyber insurance varied. Leading the way were companies with a lot of consumer data who are filling gaps in traditional coverage and looking to lessen financial harm and mitigate reputational damage. Additionally, companies who are third party vendors with required contractual obligations also sought more coverage to be in compliance. No business clients of any of the brokers surveyed chose to decrease their coverage at renewals while 67 percent said that clients were maintaining their current level of coverage.

Businesses are increasingly purchasing stand-alone policies in an effort to more holistically augment their evolving cyber risk strategy, rather than relying on embedded coverage.
Sixty-four (64) percent of survey participants reported that their clients have stand-alone cyber policies. The cyber insurance market is evolving in two segments. As one broker described it, “there are those businesses that buy cyber insurance as part of their property/casualty program (limited coverage, but some coverage), and those businesses that see a true exposure that buy it mono-line.”

Recent high-profile cyber losses are driving large companies in high-target industries to alter their approach to cyber risk management from one that focuses primarily on prevention to a comprehensive strategy across the enterprise that involves assessing, managing, and responding to cyber risks.
Of brokers’ clients that have enterprise risk management programs, 33 percent now include and properly address cyber risk.

Cyber Insurance Selling Behavior

Despite challenges, the developing cyber insurance market is expected to remain favorable and expand.
There are new insurers and capacity. Carriers, brokers, and modeling firms are partnering with one another as well as with cyber security firms to drill down deeper on exposures. Broader coverage is being developed and the blending of risk transfer with other services is helping in that.

The average cyber policy limit is $2.4 million while the average largest limit brokers had placed was $50.7 million. A $500 million tower was the largest reported.
Brokers are not experiencing any capacity issues in the relatively mature primary market for basic cyber liability and data breach coverage products. However, when working upstream in the cyber insurance market which is fraught with complexity and a need for more comprehensive solutions, one broker summarized, “real large customers have to buy a lot of layers to get large limits. Frankly, I don't think anybody can truly buy enough limits.”

Insurance carriers are struggling to discover how to profitably assume risk.
The market is devoid of real-time data about cyber incidents’ causes and effects. This combined with the lack of loss experience is making the already difficult task of gauging virtual risk even harder. This limits both the spread of coverage and type of cyber products and capacity the carriers offer. Brokers, in turn, see material capacity issues coming.

Premium pricing is mostly flat right now.
Fifty-six (56) percent of survey participants claimed that prices were flat, 28 percent indicated an uptick in pricing and 16 percent experienced a dip. Broker experience varied by client type and revenue size with health care and retail popping out as the industries seeing hardening in the market.

Confusion about what is covered and what is excluded in a cyber policy is the chief concern of brokers right now.

Seventy-one (71) percent of brokers believe that there was little to no clarity about what is and is not covered. Much rests with the individual broker's ability to grasp exposures and coverage nuances and be able to intelligently discuss these with individual clients whose interest levels vary greatly. The two major points of contention are lack of a standard terminology and difficulty in spotting exclusions.

The Council's Cyber Insurance Market Watch is released on a biannual basis. The next survey will be released in March 2016.